Hohe Anforderungen an MSSPs

SIEM als Basis für Managed Security

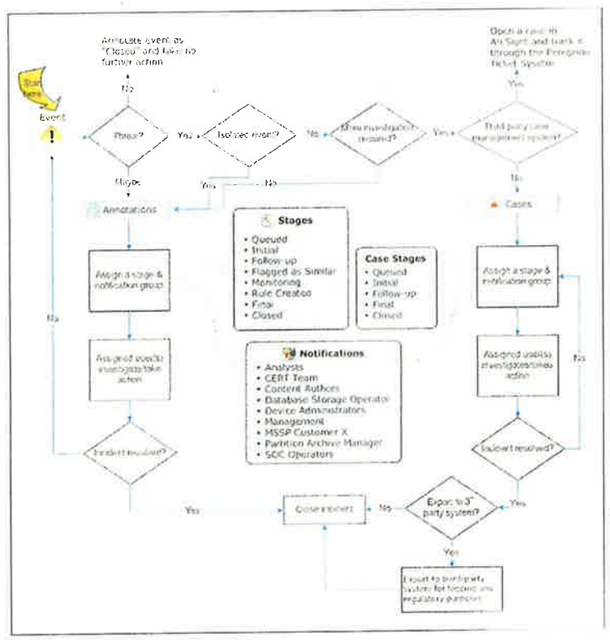
Der Leistungsumfang und die Effizienz eines MSSPs (Managed-Security-Service-Provider) hängen in hohem Maße von der eingesetzten SIEM-Lösung ab (Security-Information- and Event-Management). Entsprechend hoch sind die Anforderungen an solch eine Lösung. Dieser Beitrag beschreibt, auf welche Aspekte Security-Dienstleister und deren Kunden achten sollten.

Managed-Security-Services sind die Summe der Sicherheitsleistungen für einen Applikationsbetrieb. Sie umfassen eine Vielzahl an Maßnahmen, darunter Application-Security-Services (inklusive Firewall, Virenschutz und Spam-Filter), Network-Security-Services (wie Intrusion Detection/Prevention, VPN) sowie Vulnerability-Services (Scans, Threat and Vulnerability Information, Computer Emergency Response Team, kurz CERT).

Betriebsseitig umfasst der MSSP-Ansatz die Basisleistungen Incident-, Problem-, Change- und Service-Management. Managed-Security-Services sind somit eine Gesamtlösung in der IT-Security, die umfassende Einzelleistungen bündelt und sich an den Geschäftsprozessen orientiert. Heute sind die genutzten Techniken soweit ausgereift, dass eine solche Gesamtlösung einfach umsetzbar ist.

Im Rahmen einer Aufklärung von Sicherheitsvorfällen oder einer Zertifizierung müssen Unternehmen einen sicheren IT-Betrieb nachweisen. Diese Forderung wird durch Sicherheitsstandards beispielsweise von Kreditkartenherausgebern mit dem Payment Card Industry Data Security Standard (PCI DSS) adressiert. Eine Kernforderung im Rahmen einer Zertifizierung nach PCI DSS an den IT-Betrieb ist die Nachvollziehbarkeit der implementierten Sicherheitsmaßnahmen. Dies wird durch aktive und reaktive Maßnahmen erreicht. Die aktiven Maßnahmen sehen ein Echtzeit-Monitoring der Logfiles der beteiligten IT-Systeme und monatliche Compliance-Berichte vor. Bei einem Sicherheitsvorfall leitet ein CERT die reaktiven Maßnahmen im Rahmen eines Incident-Managementprozesses ein.

Technisch betrachtet handelt es sich bei den betroffenen Daten um verschiedene Logdatenformate von IT-Systemen wie Router, Firewalls, Server, Clients, IDS/IPS-Geräten (Intrusion Detection/Prevention System) und Virenscannern. All diese Systeme produzieren im Sekundentakt Logfiles, die es automatisch zu sammeln zu vergleichen, auszuwerten und revisionssicher zu speichern gilt. Heute ist es möglich, aus den weltweit verteilten Logdaten die Compliance-relevanten Daten (Compliance: Einhaltung von Vorschriften) zu extrahieren und zu verwalten. Für diesen automatisierten Prozess setzt ein Unternehmen sinnvoller Weise ein SIEM-System ein.



MSSPs erbringen die IT-sicherheitsbezogenen Services gemäß klar definierter Arbeitsabläufe
Quelle: Lufthansa Systems

Hohe Messlatte für SIEM-Systeme

Die Anforderungen an ein SIEM-System sind so vielfältig, dass sich in den letzten drei Jahren ein sehr aktiver Markt eröffnet hat, in dem viele große Softwarehersteller vertreten sind. Die Lösungen haben nun die Reife, um die aktuellen Herausforderungen im Bereich Managed-Security-Services zu erfüllen. Wer sich für ein SIEM-System entscheidet, sollte aber unbedingt bestimmte Kriterien beachten. Wesentlich für die ideale Lösung sind die Architektur und das Reporting sowie betriebliche Aspekte des Anbieters.

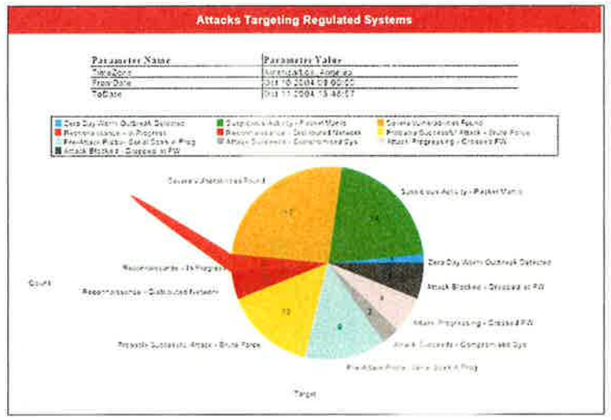
Die erste Entscheidung sollte zwischen hardware- oder softwarebasierter Lösung fallen. Vorteil der hardwarebasierten Variante ist die höhere Verarbeitungsgeschwindigkeit und schnelle Integration. Die softwarebasierte Lösung dagegen bietet durch die offene Architektur mehr Möglichkeiten zur Integration von Fremdsystemen und einen standardisierbaren IT-Betrieb.

Die Leistungsfähigkeit von SIEM-Systemen wird in Events pro Stunde gemessen, die die Datenbanken im Hintergrund verarbeiten. Je nach Budget und Komplexität der zu schützenden Infrastruktur muss ein SIEM-System eine bestimmte Anzahl Events pro Stunde verarbeiten. Lufthansa Systems zum Beispiel setzt eine SIEM-Lösung ein, die für rund zwei Millionen Events pro Stunde ausgelegt ist, die in Echtzeit abgefragt und verarbeitet werden.

Gleichzeitig sollte kein statisches System angeschafft werden, da sich Geschäftsprozesse ändern und neuen Märkten und Geschäftsfeldern anpassen. Das SIEM-System sollte daher erweiterbar und anpassungsfähig sein und gleichzeitig die Möglichkeit bieten, mandantenfähig neue Systeme oder Kunden hinzuzufügen. Ein weiteres wichtiges Kriterium ergibt sich aus der Anzahl der IT-Systeme, die an eine SIEM-Lösung angeschlossen werden. In der Regel hat jede große Produktfamilie ihr eigenes Logdatenformat. Dieses Format muss das SIEM-System verarbeiten und auswerten können. Falls das System ein Logdatenformat nicht unterstützt, sollte ein gut dokumentiertes Software Development Kit (SDK) vorhanden sein, mit dem ein Unternehmen eigene Anschlüsse an das SIEM-System programmieren kann.

Relevante Daten sollten zentral vorgehalten werden, da dies eine optimale Backup- und Recovery-Strategie zulässt und eine Korrelation von Daten in Echtzeit über Systemgrenzen ermöglicht. Dies ist vor allem für verteilte Angriffe über die gesamte IT-Infrastruktur wichtig, da sich alle Daten auf einem zentralen Bildschirm (dem „Dashboard") zusammenführen und interpretieren lassen. Der Datentransfer von den Satellitensystemen zum Zentralsystem muss verschlüsselt und authentifiziert erfolgen, damit Angreifer die übertragenen Daten nicht verändern können.

Treffen Events ein, nimmt das SIEM-System nach der Korrelation der Daten intern eine Priorisierung nach definierten Kriterien vor. Sie wirkt sich auf den durchzuführenden Prozess aus und kann von einer „Watch List" bis zum Senden einer Alarmierungs-SMS an den Systemverantwortlichen und das Starten des entsprechenden ITIL-Prozesses reichen. Bei nicht direkt erkennbaren Angriffen oder solchen, die sich über einen langen Zeitraum erstrecken, muss die Option bestehen, historische Daten zur Angriffserkennung heranzuziehen. Ein Beispiel dafür ist eine Malware, die auf einem Client erst nach einer gewissen Zeit aktiv wird.



Ein SIEM-Dashboard liefert einen Überblick über Zahl und Zusammensetzung sicherheitsrelevanter Vorfälle
Quelle: Lufthansa Systems

Das Reporting einer SIEM-Lösung muss Berichte online und offline anbieten und automatisiert in einem bestimmten Zeitfenster erstellen. Der Inhalt der Reports sollte auf den Verwendungszweck abgestimmt sein. Für einen Wirtschaftsprüfer, der zum Ende des Bilanzierungsjahres die IT-Risiken bewertet, müssen die Daten im SIEM-System ebenso aufbereitet werden können wie für einen Auditor, der das IT-System gegenüber seinen Anforderungen prüft.

Betriebliche Aspekte

Besonderes Augenmerk ist auf die Betriebs- und Datensicherheit sowie die Mandantenfähigkeit der eingesetzten Lösung zu legen. Schließlich ist das SIEM-System in kritische Prozesse wie den Incident-Managementprozess eingebunden, und bei Nutzung und Betrieb sind die Rollen verteilt. Zentrale Komponenten wie Datenbank und Applikationsserver müssen in die unternehmenseigenen Hochverfügbarkeitsszenarien passen. Ein weiterer wichtiger betrieblicher Aspekt ist die Nicht-Veränderbarkeit und Sicherheit der im SIEM gespeicherten Daten. Falls Daten aus dem System gerichtlich Verwendung finden sollen, muss nachweisbar sein, dass die Original-Logdaten unverändert in das SIEM-System übertragen wurden. Dafür setzen viele Hersteller digitale Signaturen ein, um den exakten Zeitpunkt der Datenerhebung festzuhalten. Auch eine intuitive Benutzeroberfläche ist wichtig. Schließlich arbeiten unterschiedliche Benutzergruppen wie CERT, SIEM-Administrator oder Security Operation Center (SOC) mit dem System.

SIEM-Lösung als Klammer

Eine SIEM-Lösung bildet die Klammer um die Managed-Security-Services und beantwortet die Frage: „Wie sicher waren die IT-Systeme im vergangenen Monat?" Wenn die prüfungsrelevanten Daten der IT-Systeme einem Wirtschaftsprüfer in einem Report aufbereitet zur Verfügung stehen, verringert dies den Aufwand der Prüfung. Zudem macht dies dem Prüfer wie auch dem Geprüften die Leistungen der IT-Security anschaulich. Gleichzeitig spart der Einsatz eines solchen Systems Zeit und Kosten.

Christian Kaltenhofer/wg

Christian Kaltenhofer ist IT-Architekt bei Lufthansa Systems.

Anbieterübersicht: Managed Security Service Provider

Anbieter	Telefonnr.	Managed Security Services: Bedrohungsanalyse/Vulnerability Scans	Systemüberwachung/-management	Sicherheitskonzepte/-beratung	Evaluierung der Gesetzeskonformität	Firewall/VPN	IDS/IPS	Anti-Virus	Verschlüsselung	Identity-Management/AAA	Spam-Filter	Content Filtering	Backup/Hochverfügbarkeit	E-Mail-Sicherheit/-Archivierung	WLAN-Absicherung	Datenschutzprüfung	Komplett-Outsourcing	andere	Service und Support: Support nur zu Geschäftszeiten	24x7-Hotline	24x7-Vor-Ort-Service	24x7-Monitoring (SOC)	eigenes Emergency Response Team	Direktleitung zu Anti-Virus-Anbieter	Zertifiziert für Security-Produkte der Hersteller	... sowie weiterer Hersteller	Dienstleister nicht an einzelne Hersteller gebunden	Angaben zum Unternehmen: Gründungsjahr	Zahl der Mitarbeiter	ISO27001-/ISO17799-zertifiziert	ISO9001-zertifiziert	andere Security-Zertifikate	international tätig	deutschlandweit tätig	ausschließlich regional tätig
Abacom	05271/967130	●	●	●		●		●		●	●	●		●				●	●	●	●	●			Secure Computing, Juniper, Borderware	●	●	1995	18				●	●	
Arago	069/40568104	●	●	●			●	●		●	●	●		●			●			●	●	●			Genua		●	1995	65				●		
Arxes	0221/96486-140	●	●	●	●	●	●	●		●	●	●		●			●			●		●	●		Check Point, Symantec, RSA	●		1990	1300					●	
Antispameurope	0511/2609050								●		●		●	●						●		●	●	●			●	2004	16				●	●	
Axians	02203/10250		●	●		●		●		●			●							●	●	●	●		Cisco/Ironport, Juniper, Phion	●	●				●	●		●	
BCC	0531/20840		●	●		●		●	●	●	●	●		●						●	●	●			Cisco, Secure Computing, Trend Micro	●		1997	120	●	●			●	
Bell	0721/662499363	●	●	●		●	●	●	●	●	●	●	●	●	●					●	●	●	●		Astaro, Juniper, Enterasys	●	●	1993	35				●		
BSSE	06183/92995-0		●	●			●	●		●	●	●	●							●	●		●		Microsoft, Gateprotect		●	1990	13				●	●	
BT	089/26008574	●	●	●	●	●	●	●	●	●	●	●	●	●	●					●		●	●		Cisco, Siemens	●	●		1450	●	●	●	●	●	
CI-Gate	0471/8062080		●	●		●	●	●	●	●	●	●	●				●			●		●					●	2003	12				●	●	
Circular	0711/78717-0	●	●	●	●	●	●	●	●	●	●	●	●	●	●					●	●	●			Juniper, Cisco, Trend Micro	●		1995	60					●	
Claranet	069/408018-0		●		●		●	●		●		●	●							●		●						2000	100			●	●		
Clearswift	040/239990			●			●		●	●	●	●								●	●							1982	260			●	●		
Comco	0231/47644-0	●	●	●	●	●	●	●	●	●	●	●	●	●	●					●	●	●			Juniper, Extreme, Kaspersky	●	●	1998	35					●	
Computacenter	02273/597-0	●	●	●	●	●	●	●	●	●	●	●	●	●	●					●	●	●		●			●	1981	4000	●	●		●	●	
Concipia	0800/26624742	●	●	●	●	●	●	●	●	●	●	●	●	●	●					●	●	●	●		Sonicwall		●	2000	15			●	●		
Cosus	07724/9386-935	●	●	●	●	●	●	●		●	●	●	●	●	●					●	●			●	F-Secure, Clearswift, Symantec	●	●	1990	36				●	●	
Damovo	0211/87554173	●	●	●	●	●	●	●	●		●	●	●	●						●	●	●			Cisco, Nortel, Check Point								●	●	●
Dawin	02241/397198-0	●	●	●		●		●		●	●	●	●	●								●		●			●	2003	15						●
Dr. Morawietz	06251/1058-0	●	●	●	●	●	●	●	●	●		●	●	●		●	●					●			Microsoft, Kaspersky, GFI			1990	22				●		●
Eggenet	05251/8988-80	●	●	●		●	●	●		●	●	●					●			●	●	●			Sonicwall, Juniper, Secure Computing	●	●	1996	30						●
Eleven	030/520056-273							●		●		●			●			●		●		●			Eleven, Avira			2001	35				●		
Ete	05401/867520	●	●	●	●	●	●	●	●	●	●	●	●	●	●					●	●	●			Cisco, Watchguard, Reddoxx	●	●	1979	20						●
Euromicron	07243/524948		●	●		●	●		●	●	●	●	●	●	●						●	●	●		Enterasys, Astaro, Zyxel	●	●	1987	250		●	●			●
F-IT	07531/81996-0	●	●	●	●								●		●	●										●	●	2003	6				●		
Fortinet	069/710423535	●	●	●	●	●	●	●	●		●	●	●	●						●	●		●	●				2000	1025		●	●	●	●	
F-Secure	089/7874670				●	●	●		●											●		●						1988	600				●		
GCT	0800/2255428	●	●	●		●	●	●		●	●		●		●							●			Sonicwall			1989	12						●
Genua	089/991950-0		●	●		●	●	●	●		●	●								●		●			Genua			1992	100			●	●		
G&M	06851/8007824	●	●	●	●	●	●	●	●		●	●	●	●						●					Sonicwall, GFI			2006	8						●
HL Komm	0341/8697-0		●	●		●		●	●		●	●	●							●	●	●			Cisco		●	2000	90						●
IAD	0361/65930-0		●	●		●		●	●			●		●													●						●		●
Ikarus	0043/1/58995-0			●			●		●	●					●	●												1986	40				●		
IKU	0681/96751-0		●	●		●		●		●				●											Novell, Avira, Sponts	●	●	2006	8						●
Interoute	030/25431-1721		●			●	●	●		●	●	●					●				●	●	●		Cisco, Check Point, IBM ISS	●		1995	970	●		●	●	●	

Anbieter	Telefonnr.	Managed Security Services: Bedrohungsanalyse/Vulnerability Scans	Systemüberwachung/-management	Sicherheitskonzepte/-beratung	Evaluierung der Gesetzeskonformität	Firewall/VPN	IDS/IPS	Anti-Virus	Verschlüsselung	Identity-Management/AAA	Spam-Filter	Content Filtering	Backup/Hochverfügbarkeit	E-Mail-Sicherheit/-Archivierung	WLAN-Absicherung	Datenschutzprüfung	Komplett-Outsourcing	andere	Service und Support: Support nur zu Geschäftszeiten	24x7-Hotline	24x7-Vor-Ort-Service	24x7-Monitoring (SOC)	eigenes Emergency Response Team	Direktleitung zu Anti-Virus-Anbieter	Zertifiziert für Security-Produkte der Hersteller	... sowie weiterer Hersteller	Dienstleister nicht an einzelne Hersteller gebunden	Angaben zum Unternehmen: Gründungsjahr	Zahl der Mitarbeiter	ISO27001-/ISO17799-zertifiziert	ISO9001-zertifiziert	andere Security-Zertifikate	international tätig	deutschlandweit tätig	ausschließlich regional tätig
Interxion	069/40147-0		●				●												●	●		●						1998	200	●					
ISM	0381/375730									●									●						Microsoft CP			1998	30				●	●	
ITC	0451/48434-0	●	●	●			●	●		●									●			●			Sonicwall, Kaseya, Citrix	●		1997	15				●	●	
JZB	089/945118115		●	●	●		●	●		●										●	●	●	●					1994	600	●	●		●		
Lambdanet	0511/84881129		●	●			●	●		●		●			●					●		●						1999	100	●					
LEW Telnet	0821/328-1400				●		●					●	●						●	●		●			Cisco, Check Point, Sonicwalll	●		1997	70						●
Linbit	0043/1/81782020			●	●		●			●	●		●	●						●	●	●						2001	17				●		
McAfee	089/37070	●			●				●			●	●		●					●			●	●	McAfee			1996	80				●		
Messagelabs	089/189443990	●			●	●			●	●		●	●		●				●	●			●				●	1999	500	●			●	●	
Mivitec	089/420797870	●	●	●	●	●	●	●	●	●	●	●	●	●	●		●			●	●	●	●				●			●			●	●	
Network Engineering	06232/60680	●	●	●		●	●	●	●	●	●	●	●	●	●	●	●		●	●		●	●	●	F-Secure, Trend Micro, Secure Computing		●	1998	14				●		
Netzwerk Not	0228/9090200	●	●	●		●	●	●	●	●	●	●	●			●				●	●	●	●	●	Secure Computing, Phion, Trend Micro	●	●	2003	12				●	●	●
NIIT	0711/71917-441	●	●	●	●	●	●	●	●		●	●		●		●	●	●		●		●		●	Netiq, F-Secure, Sonicwall	●		1981	60	●	●		●	●	
Orange Business Services	06196/962-0	●	●	●		●	●	●	●	●	●	●	●	●		●				●	●	●	●	●	Check Point, Juniper, Fortinet	●			354				●		
Pallas	02232/18906-0	●	●	●		●	●	●		●	●	●	●	●	●					●	●	●		●	Sonicwall, Check Point		●	1991	15				●	●	
Panda Security	02065/961-0	●	●	●				●	●			●	●			●				●				●				1990	2000				●		
Percomp-Verlag	040/696281600	●		●		●		●						●		●	●			●				●	F-Secure, M-Privacy, Mainskill	●		1989	12						●
Q-Soft	0361/7785820	●	●	●		●	●	●	●	●	●	●	●	●						●		●	●	●	Cisco, RSA, Trend Micro	●	●	1990	60		●				●
Qualys	089/97007146	●			●															●				●	Qualys		●	1999	200				●	●	
Retarus	089/55280			●	●			●	●		●		●							●		●					●	1992	160					●	
R-Tec	02339/9182-920	●	●	●	●	●	●	●	●	●	●		●		●					●	●	●			Check Point, Secure Computing, Juniper	●	●	1996				●		●	●
Sandata	0911/95230	●	●	●	●	●	●	●	●	●	●	●	●	●	●					●	●			●	Symantec, Clearswift, Sonicwall	●	●	1981	225				●	●	
Schweickert	06227/3086-00	●	●	●	●	●	●	●	●	●	●	●	●	●	●					●	●	●			Check Point, Aladdin, Enterasys		●	1992	80					●	●
SHE	0621/5200199	●	●	●	●	●	●	●	●	●	●	●	●	●	●					●	●	●	●	●	Check Point, Aladdin, RSA	●		1987	85				●	●	●
Sirrix	0234/610071-0	●	●	●		●			●	●			●	●	●													2001	45				●	●	●
Spacenet	089/32356-0	●	●	●		●	●	●	●	●	●	●	●	●		●				●	●	●	●		Juniper, Citrix, Kobil			1993	70	●				●	
Symantec	089/66410300	●	●	●		●	●	●		●		●				●				●	●	●					●	1982	17.500	●			●	●	
Synectico	02161/931490			●		●		●		●	●				●					●		●		●	Sonicwall, Sophos, Secure Computing	●	●	2003	12				●	●	
Telcat Multicom	05341/218598	●	●	●	●	●	●	●		●	●	●	●	●	●	●	●	●		●			●	●	Sonicwall, Websense, Kaspersky	●	●	1983	485		●	●		●	
Telco Tech	03328/430810	●	●	●		●	●	●	●		●	●	●	●		●	●			●	●	●	●		Liss Security Systems		●	1993	25				●		●
T-Systems	0800/87978367	●	●	●	●	●	●	●	●		●	●	●	●						●	●	●	●	●	Blue Coat, Check Point, Trend Micro			2000	56.500	●			●	●	●
Tulock	0681/940000-0	●	●	●	●	●	●	●	●		●	●	●	●	●					●		●			Sonicwall, Qualys			2007	6				●	●	●
Vanco	06102/785555		●	●		●	●	●	●	●	●	●								●	●	●					●	1989	700					●	●
Vater	0431/799660	●	●	●	●	●	●	●	●	●	●	●	●	●	●							●	●	●	Cisco, Trend Micro		●	1997	250		●	●		●	
Verizon	069/97268-6757	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	Cisco, Juniper	●	●	1991	740	●	●	●	●		